Drone Regulatory Issues summary

S. Altini, Prof. Ioannis Pitas
Aristotle University of Thessaloniki
pitas@csd.auth.gr

Version 2.0.1

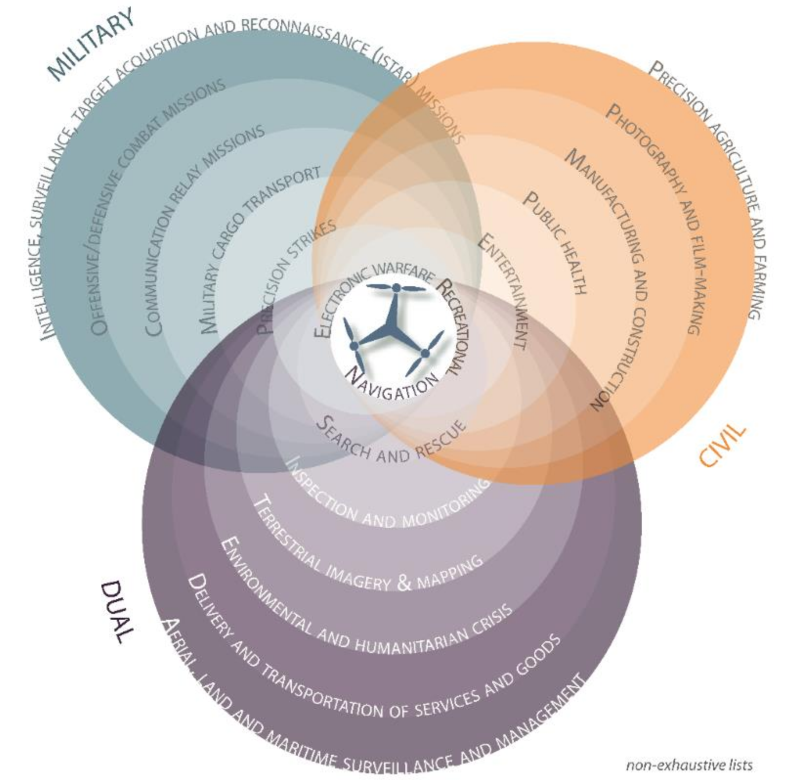
Artificial Intelligence &
Information Analysis Lab

Privacy Protection, Ethics and regulations

- **Dual use**
- Misuse avoidance & Data Security
- Data Protection
- Privacy Protection

Dual Use

- **Definition:** As dual-use products can be defined items, services, and technologies that take into account the needs of both defense and civilians. The EU controls exports, transits and brokering of dual-use items, which makes an effective contribution to global peace and security, avoiding the Mass Destruction Weapons' further proliferation.


MILITARY
Intelligence, surveillance, target acquisition and reconnaissance (ISTAR) missions
Offensive/defensive combat missions
Communication relay missions
Military cargo transport
Precision strikes
Electronic warfare
CIVIL
Precision agriculture and farming
Photography and film-making
Manufacturing and construction
Public health
Entertainment
Recreational
Navigation
DUAL
Search and rescue
Inspection and monitoring
Terrestrial imagery & mapping
Environmental and humanitarian crisis
Delivery and transportation of services and goods
Aerial, land and maritime surveillance and management
non-exhaustive lists

Source: EPRS, 2019.

Multi-purpose usage of drones

Civilian use cases

- **Emergency response**: as mobile medical, sending first aid response, necessary help without delays, supplying isolated/infected patients;
- **Cinematography/photography/filming:** ensure aerial filming, capture a scene with HD quality, reducing the needs of high cost equipment and human interaction;
- **Search and rescue**: when human presence is deemed in risk or limited, and for lost or even stranded people etc.;

Multi-purpose usage of drones

Civilian use cases

- **Natural disaster response/control:** environmental disaster relief operations, fire-fighting, humanitarian aid distribution, disaster consequences, check for injured and trapped survivors.
- **Tourism:** capture the spectacular views of touristic sights/areas of interest, amplifying the overall tourism industry;
- **Inspecting infrastructure:** for wear and damage;
- **Other cases**: farming, delivery, sports, help in identifying individuals using the GPS locations/MAV addresses.

Multi-purpose usage of drones

Police use cases

- **Track down suspects:** aerial surveillance as cheaper and more flexible mean than a helicopter;
- **Enhance traffic efficiency:** offering accelerated response and road conditions identification;
- **Crisis management:** serve as hot spots or bases, gathering messages sent by affected human in case of natural disaster (earthquakes, floods) or in terrorist attack may act as Access Point;
- **Surveillance purposes:** detect hidden suspicious targets, on account to their ability ti identify humans from biometric data.

Multi-purpose usage of drones

Military use cases

- intelligence, reconnaissance, and surveillance missions;
- combat missions through the use of armed drones;
- real-time protection of troops;
- direct target eradication, using laser-guided missiles against terrorist;
- covert aerial surveillance and reconnaissance, on account of the ability/capability to remain undetected of radar systems;
- intercept of footage in an attempt “to thwart a domestic terror attacks”;
- underwater “surveillance and reconnaissance operations”.

Dual use: Risks for drones

Risks are mainly related to:

- **Export license**
  - Refusal of export license;
  - Delivery of export license (delay);
  - Provision of incorrect/missing information, regarding export license;
  - Not required export license, however needed.
- **End-use statement update**
  - COTS component required;
  - COTS must be mentioned in end-use statement/export license, granted by manufacturer;
  - Updated end-use statement/export license, compliant to regulations.
- **Transfer of MULTI DRONE prototype**
  - Export license required, given by EU authority;
  - Updated end-use statement/export license required.

Privacy Protection, Ethics and regulations

- Dual use
- **Misuse avoidance & Data Security**
- Data Protection
- Privacy Protection

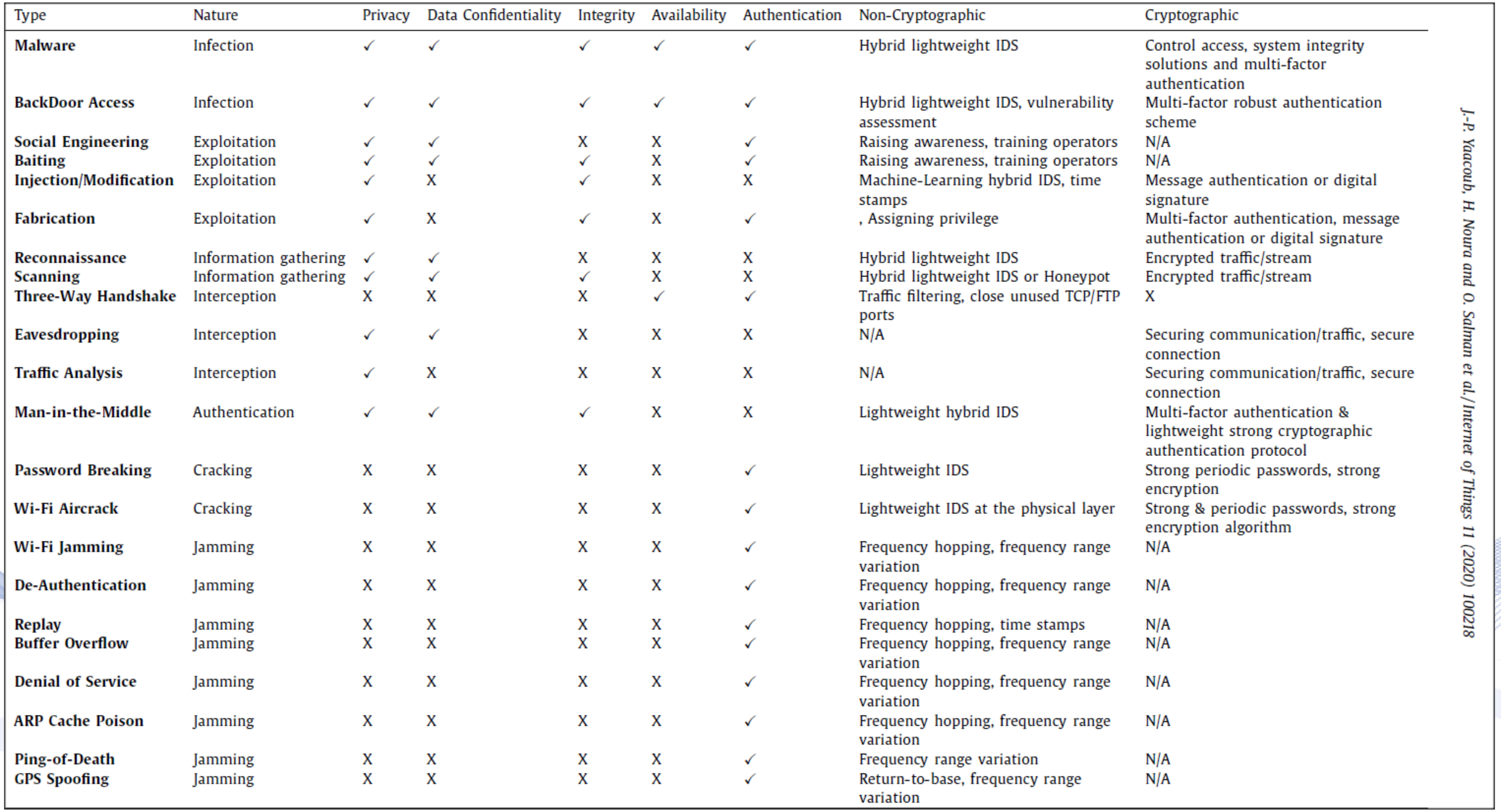
Drones: Security and Safety aspects

Classification of drones' communications:

- **Drone-To-Drone (D2D):** Peer-to-Peer (P2P) communication expose system in various P2P vulnerabilities and attacks (D-DoS, sybil attacks). Machine Learning optimizes the wireless communication system, but yet not reached the standardized status.
- **Drone-To-Ground station (D2GS):** communication used protocols (Bluetooth/Wi-Fi)/public and unsecure/using single factor authentication. Vulnerable functioning to active (man-in-the-middle) and passive (eavesdropping) attacks.
- **Drone-To-Network (D2N):** through this type, the given option is to choose the network, using the required security level, including cellular communications that, also, need to be secured.
- **Drone-To-Satellite (D2S):** communication used to send real-time coordinates via GPS. Satellite communications are considered as secure/safe, exhibit substantial cost/maintenance requirements.

Drones: Security and Safety aspects

Drones counter-drones cyberattacks



Type	Nature	Privacy	Data Confidentiality	Integrity	Availability	Authentication	Non-Cryptographic	Cryptographic
Malware	Infection	✓	✓	✓	✓	✓	Hybrid lightweight IDS	Control access, system integrity solutions and multi-factor authentication
BackDoor Access	Infection	✓	✓	✓	✓	✓	Hybrid lightweight IDS, vulnerability assessment	Multi-factor robust authentication scheme
Social Engineering	Exploitation	✓	✓	X	X	✓	Raising awareness, training operators	N/A
Baiting	Exploitation	✓	✓	✓	X	✓	Raising awareness, training operators	N/A
Injection/Modification	Exploitation	✓	X	✓	X	X	Machine-Learning hybrid IDS, time stamps	Message authentication or digital signature
Fabrication	Exploitation	✓	X	✓	X	✓	, Assigning privilege	Multi-factor authentication, message authentication or digital signature
Reconnaissance	Information gathering	✓	✓	X	X	X	Hybrid lightweight IDS	Encrypted traffic/stream
Scanning	Information gathering	✓	✓	✓	X	X	Hybrid lightweight IDS or Honeypot	Encrypted traffic/stream
Three-Way Handshake	Interception	X	X	X	✓	✓	Traffic filtering, close unused TCP/FTP ports	X
Eavesdropping	Interception	✓	✓	X	X	X	N/A	Securing communication/traffic, secure connection
Traffic Analysis	Interception	✓	X	X	X	X	N/A	Securing communication/traffic, secure connection
Man-in-the-Middle	Authentication	✓	✓	✓	X	X	Lightweight hybrid IDS	Multi-factor authentication & lightweight strong cryptographic authentication protocol
Password Breaking	Cracking	X	X	X	X	✓	Lightweight IDS	Strong periodic passwords, strong encryption
Wi-Fi Aircrack	Cracking	X	X	X	X	✓	Lightweight IDS at the physical layer	Strong & periodic passwords, strong encryption algorithm
Wi-Fi Jamming	Jamming	X	X	X	X	✓	Frequency hopping, frequency range variation	N/A
De-Authentication	Jamming	X	X	X	X	✓	Frequency hopping, frequency range variation	N/A
Replay	Jamming	X	X	X	X	✓	Frequency hopping, time stamps	N/A
Buffer Overflow	Jamming	X	X	X	X	✓	Frequency hopping, frequency range variation	N/A
Denial of Service	Jamming	X	X	X	X	✓	Frequency hopping, frequency range variation	N/A
ARP Cache Poison	Jamming	X	X	X	X	✓	Frequency hopping, frequency range variation	N/A
Ping-of-Death	Jamming	X	X	X	X	✓	Frequency range variation	N/A
GPS Spoofing	Jamming	X	X	X	X	✓	Return-to-base, frequency range variation	N/A

J.-P. Yaacoub, H. Noura and O. Salman et al./Internet of Things 11 (2020) 100218

Privacy Protection, Ethics and regulations

- Dual use
- Misuse avoidance & Data Security
- **Data Protection**
- Privacy Protection

Data Security requirements

Data security

- **Data stored within drones:**
  - Data encryption, enabling access only on people with authentication.
- **Data stored in ground infrastructure:**
  - Use of technologies, including memory isolation, provided by virtualization to control access to data between applications;
  - Hacking detection: shut down/lock/erase UAV devices to prevent uncontrolled capture of personal data.
- **Data transmitted over the air**:
  - Wi-Fi/radio transmitted data are unencrypted (commercial use of drones);
  - Data protection with authentication and encryption mechanisms (IPSec protocol over LTE).
- **Data to be distributed publicly (e.g. UAV datasets)**

Data Protection issues in Drones

- **Public perceives, when drones breach privacy**: trespassing/flights above private property are forbidden. Distinction between:
  - actors, spectators, crowd;
  - public events, private events.
- **Data protection issues for AV shooting**:
  - broadcasting;
  - developing experimental databases.
- **Use of data de-identification algorithms**, during a shooting.

Privacy Protection, Ethics and regulations

- Dual use
- Misuse avoidance & Data Security
- Data Protection
- **Privacy Protection**

Privacy Protection, ethical and regulatory issues

Ethics for Drones

- **Privacy:** entrance/view of drones in private spaces; issues concerning over privacy in public settings, e.g., recording capabilities;
- **Safety:** reckless/dangerous use of drones, especially in high-crowded areas (beaches, events);
- **Enforceability:** official possibility for imposing regulations in drones;
- **Crime:** used to thievery/break-in, infringement and trespassing;
- **Nuisance:** used to harass/disrupt of individuals in public setting;
- **Professionality:** whether regulation should be differentiated for professional and recreational purposes.

Privacy protection, ethical and regulatory issues

Legal, ethical, safety, security and regulations

Technical issues

- **No-filming zones;**
- No-flight zones;
- Face de-identification;
- Protection of private spaces.

Privacy protection, ethical and regulatory issues

Legal, ethical, safety, security and regulations

Technical issues

- No-filming zones;
- **No-flight zones;**
- Face de-identification;
- Protection of private spaces.

No-flight zones

- **Static no-flight zones:** *defined by national regulations*
- ***Dynamic no-flight zones:*** *crowded areas*

- Flight supervisor can define static no-flight zones during mission planning.
- No-flight zones are automatically taken into account during mission planning and replanning.

Flight regulations

Different flight regulations are in force according to applications and UAVs types.

Restrictions

- Maximum UAV weight;
- Permitted flight radius;
- Special preconditions (e.g., licensed pilot requirements/insurance policies).

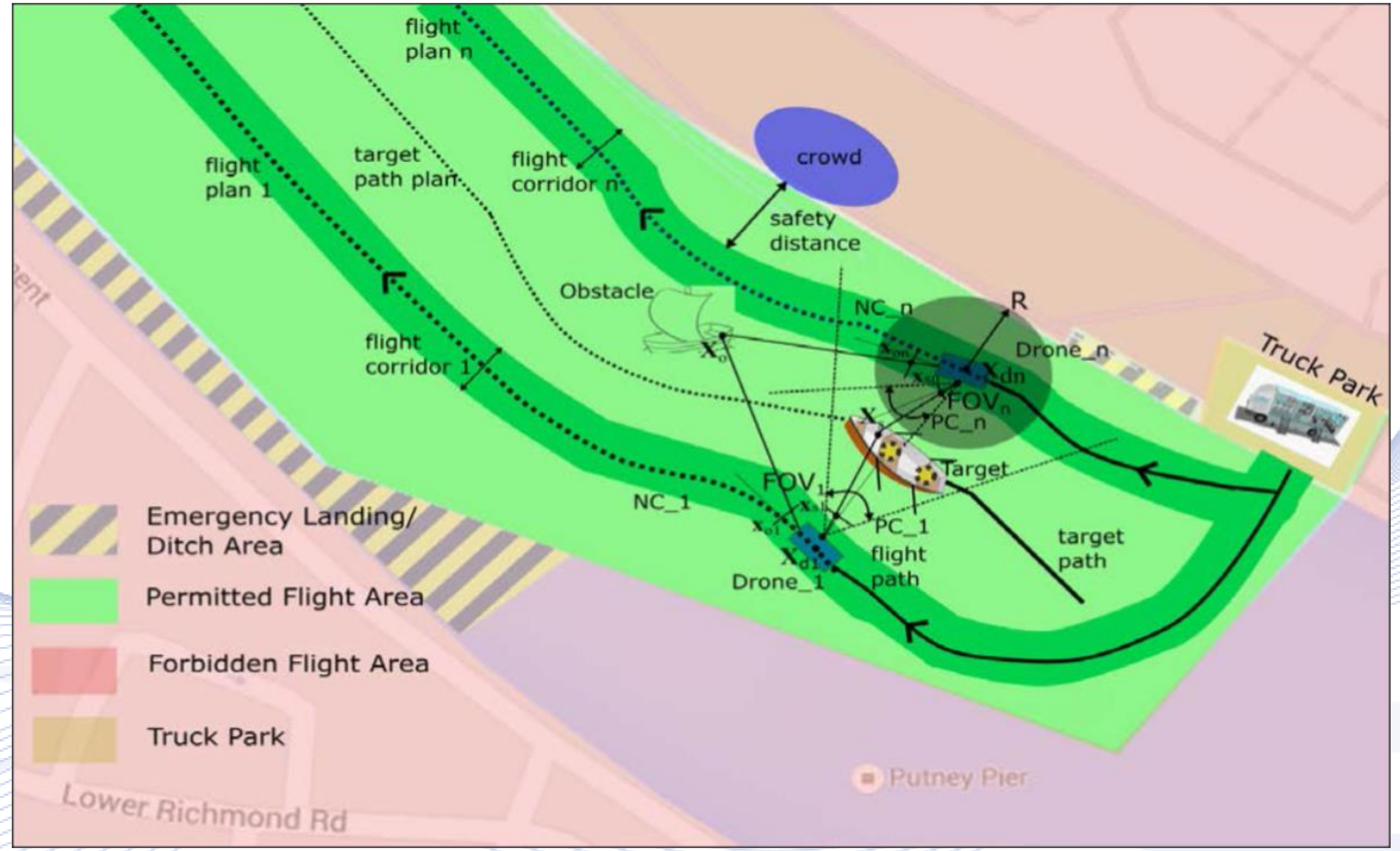
- **Notes**
  - Flight restrictions differ by country;
  - Pilot license/insurance policies may not be internationally valid;
  - Adjustment/replacement of components impacts on category classification (weight calculated by payload).

Other UAV safety issues

- **Landing sites:** Potential Landing Site Detection; Foreseen landing sites; Emergency landing site detection;
- **Flight safety:** Crowd detection and avoidance; Safety distance from crowds; Person/obstacle avoidance.

Flight safety

- **Safety distance from crowds**
  - Crowd detection and avoidance.
- **Landing sites**
  - Foreseen landing sites;
  - Emergency landing site detection;
  - Person/obstacle avoidance.



Privacy Protection, ethical and regulatory issues

Legal, ethical, safety and security, regulation

Technical issues:

- No-filming zones;
- No-flight zones;
- **Face de-identification;**
- Protection of private spaces.

Protection of private spaces

All drone operators are subjected to regulations of aviation, enforced by the CAA.

- **Keeping drone in view:** normally 500m horizontally and 400ft vertically;
- **Keeping drone away from congested areas:** any area used for residential, industrial, commercial or entertainment purposes;
- **Keeping drones at least 50m away** from individual/vehicle/building/structure not owned/controlled by the drone operator;
- **Recorded data should be ensured** that are under the Data Protection Act 1998 and/or 2018 (DPA) and General Data Protection Regulation (GDPR).

Privacy protection, ethical and regulatory issues

Legal, ethical, safety and security, regulation

Technical issues:

- No-filming zones;
- No-flight zones;
- Face de-identification;
- **Protection of private spaces.**

Q & A

Thank you very much for your attention!

More material in
http://icarus.csd.auth.gr/cvml-web-lecture-series/

Contact: Prof. I. Pitas
pitas@csd.auth.gr